INF639: Nanoelectronics for Cybersecurity

Section 2: Introduction to cryptography

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.com

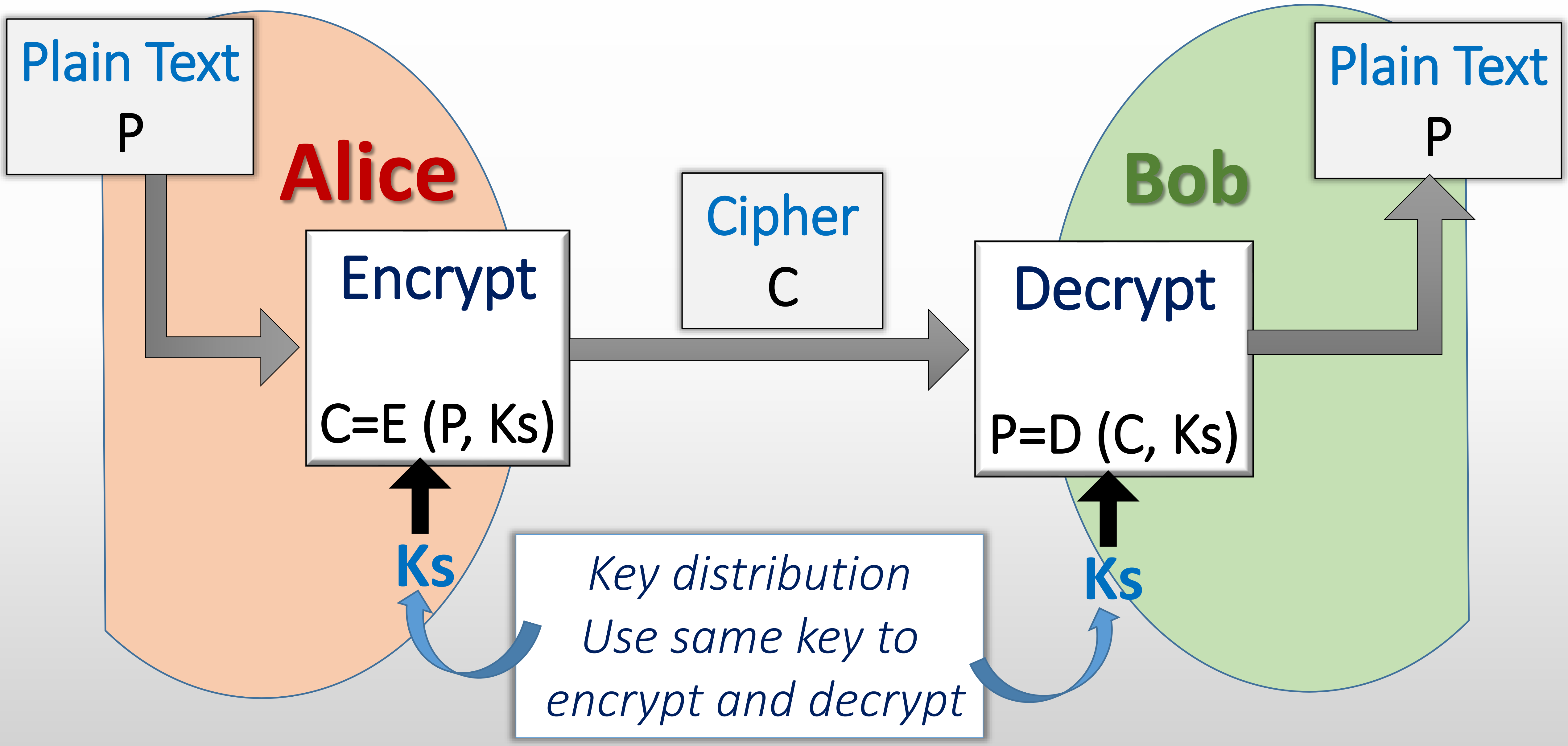
INF 639: Nanoelectronics for cybersecurity

1. From Micro to Nano-electronics
2. Introduction to cryptography
3. Public Key Infrastructure
4. Smartcards
5. Attacks on smartcards
6. MOS transistor & logic circuits
7. Biometry
8. Physical Unclonable Functions (PUF)
9. Access control and authentication
10. Flash Memory devices & security
11. Resistive RAM & security
12. Public key cryptography with PUFs
13. Sensor devices & security
14. Ternary cryptography

2. Introduction to cryptography

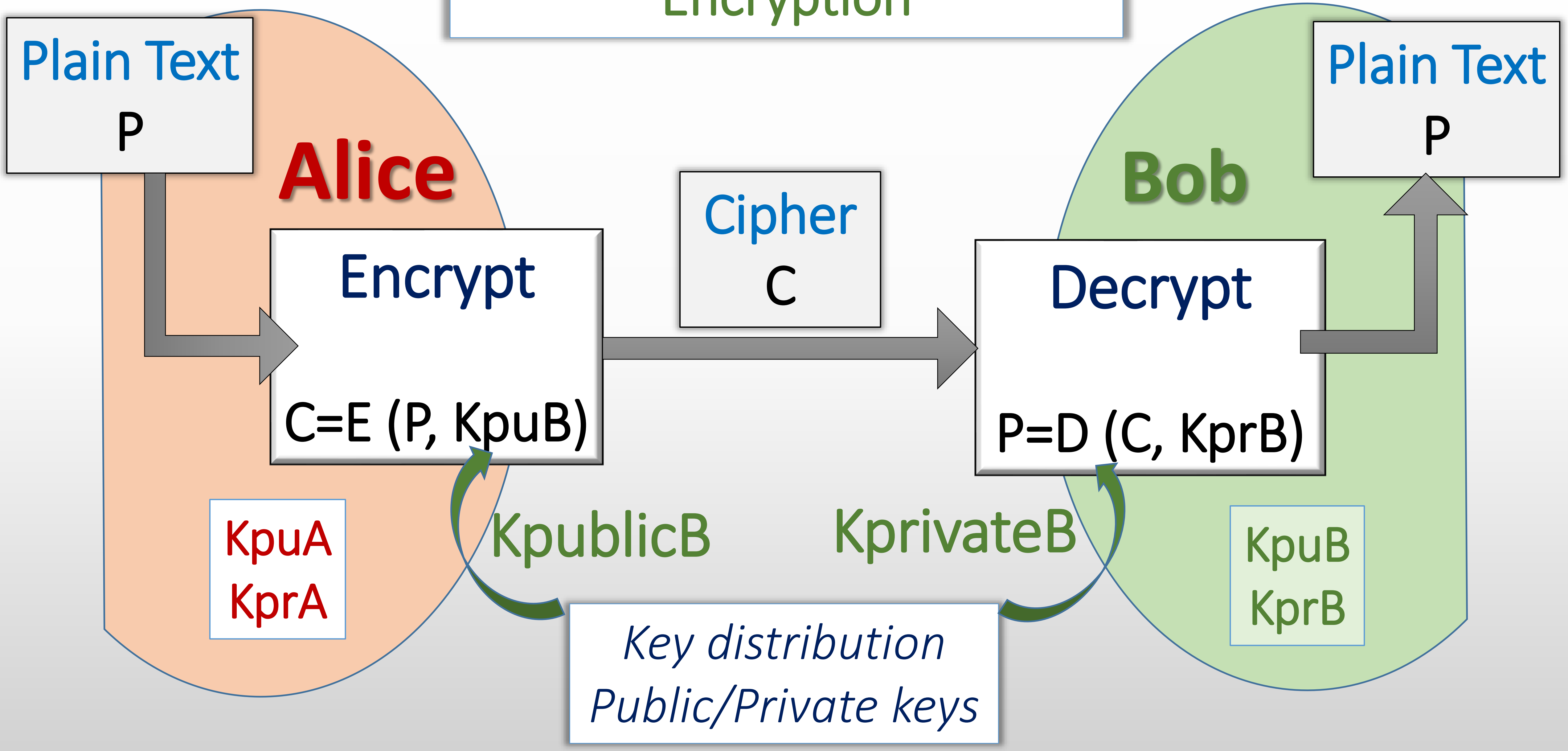
- 1- Definitions
- 2- Symmetrical cryptography
- 3- Data Encryption Standard
- 4- Advanced Encryption Standard

Symmetrical Cryptography



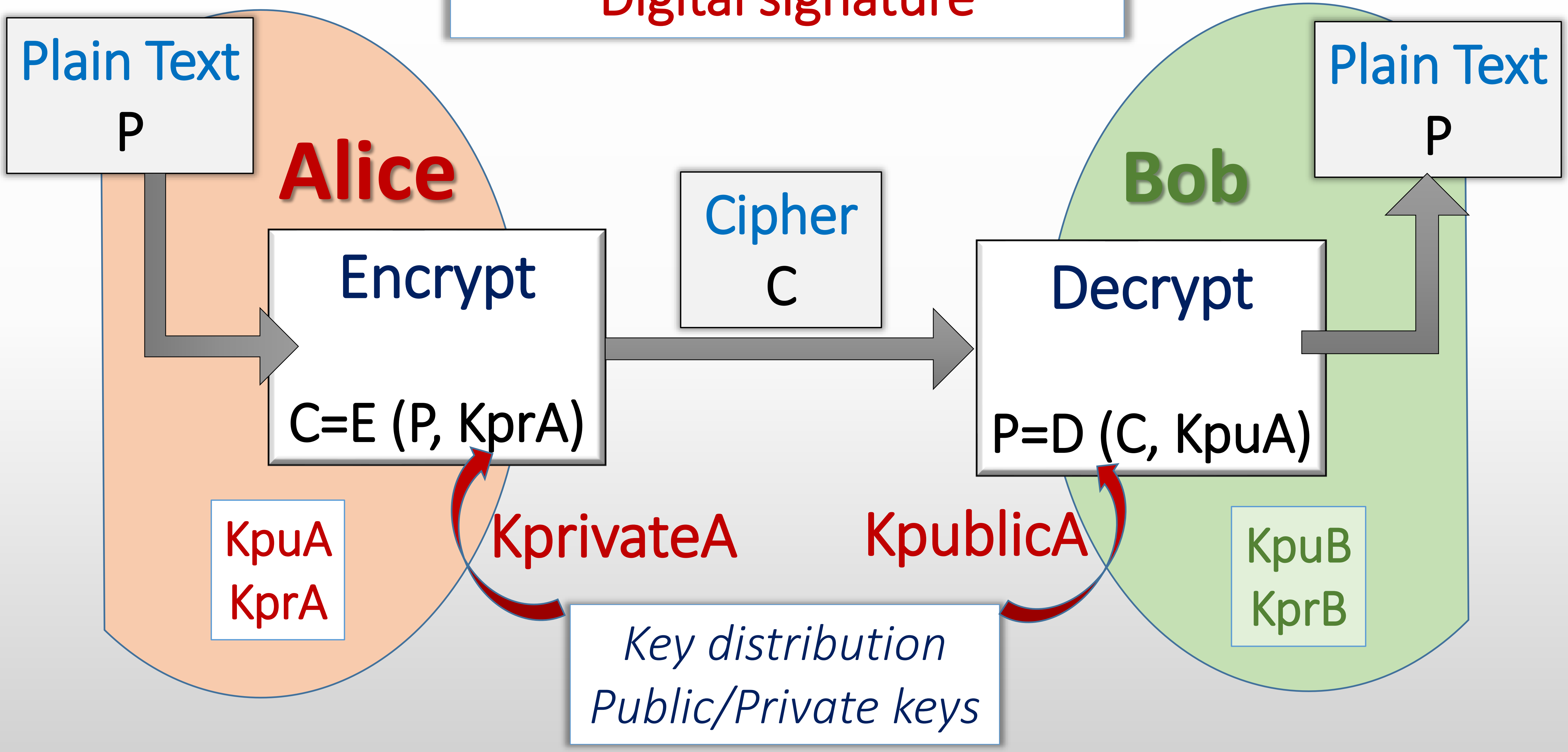
Asymmetrical Cryptography

Encryption



Asymmetrical Cryptography

Digital signature



Some Definitions -1

- ***Cryptography***: From the Greek Kryptos (hidden, covered) & -graphy (writing). The art of protecting secret information and restrict communication to a selected audience
- ***Cryptographers***: The people who create methods to effectively hide secret information.
- ***Encryption***: Conversion of a plain message into a protected message, a *cipher.*
- ***Decryption***: Conversion of a cypher into a plain message.
- ***Cryptoanalyst***: Individuals able to decrypt cyphers (also a *hacker*, or *code breakers)*.
- ***Cryptology***: the study of cryptography and cryptoanalysis.
- ***Identification***: Information describing a subject/object, that is unique
- ***Authentication***: Secret information confirming that the subject/object, is the right one.
- ***Access control***: Granting access based on secure authentication.

Some Definitions -2

- ***Cryptographic key***: Secret stream of data to encrypt/decrypt.
- **Symmetrical cryptography**: Same key is used to encrypt and decrypt messages.
- ***Asymmetrical cryptography***: Key to decrypt is different than the key to encrypt.
- ***Public key cryptography***: Asymmetrical cryptography with *public-private* keys.
- ***Cryptographic primitive***: Data stream involved in encryption such as *finger print, physically unclonable function, True Random number generator*.
- ***Biometry***: Cryptographic primitive describing human characteristic (finger print, iris, heart beat, DNA, vein, brain signals ..)
- ***Physical Unclonable Functions***: Cryptographic primitive) based on characteristics of objects or micro-components.

Some Definitions -3

- ***Quantum cryptography***: Laws of physics are used rather than mathematical algorithms. Existing methods restricted to key exchange.
- ***Post quantum computing cryptography:*** Cryptography capable to resist attacks conducted by quantum computers (or future quantum computers).
- ***Side channel analysis/attack***: Method to extract secret information while cryptography is performed
- ***Hash Function***: Function which take an input (plain text) and return it to a fixed size (smaller size) alphanumeric string, the *hash value*.
- ***Message digest***:

  Hash value that is non keyed ➔ *message integrity code*,
  or keyed ➔ *message authentication code*.
- ***Sumchecks***:

  Digest function that can flag the alteration of a message

Some acronyms -1

- ***DES***: Data Encryption System – Symmetrical algorithm.
- ***AES***: Advanced Encryption System – Symmetrical algorithm.
- ***RSA:*** Rivest Shamir Adelman – Asymmetrical algorithm.
- ***ECC:*** Elliptic Curve Cryptography – Asymmetrical algorithm.
- ***DH:*** Diffie Hellman – Asymmetrical algorithm.
- ***Entropy:*** Level of chaos – Measure the level of randomness.
- ***PUF:*** Physically Unclonable Function – Cryptographic primitive.
- ***MIC:*** Message Integrity Code – Non-keyed message digest.
- ***MAC:*** Message Authentication Code – Keyed message digest.
- ***SHS/SHA:*** Secure Hash Standard/Secure Hash Algorithm.
- ***PKI:*** Public Key Infrastructure – Deployment of asymmetrical cryptography.

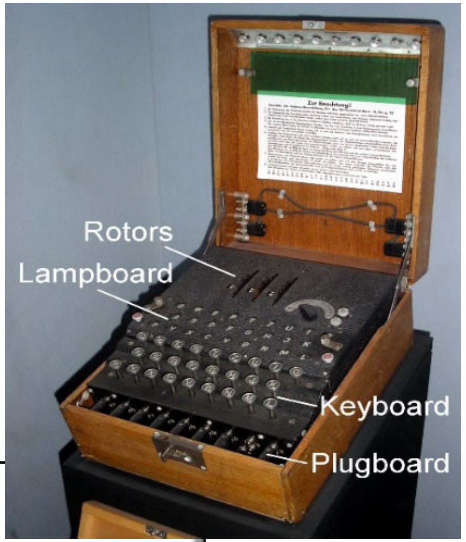
Some acronyms -2

- ***CA:*** Certificate Authority – manage digital certificate and key distribution.
- ***DSA:*** Digital Signature Algorithm.
- ***PRNG, TRNG, RNG:*** Pseudo, True Random Number Generator
- ***PGP:*** Pretty Good Privacy.
- ***S/MIME:*** Secure/Multipurpose Internet Mail Extension.
- ***SSL/TLS:*** Secure Socket Layer/Transport Layer Security.
- ***Ipsec/VPN:*** Internet Protocol Security/Virtual Private Network.
- ***SA/IKE:*** Security Association/Internet Key Exchange.
- ***DPA/SPA:*** Differential Power Analysis/Single Power Analysis.
- ***EMI:*** Electromagnetic interference

2. Introduction to cryptography

- 1- Definitions
- 2- Symmetrical cryptography
- 3- Data Encryption Standard
- 4- Advanced Encryption Standard

Symmetrical Cryptography

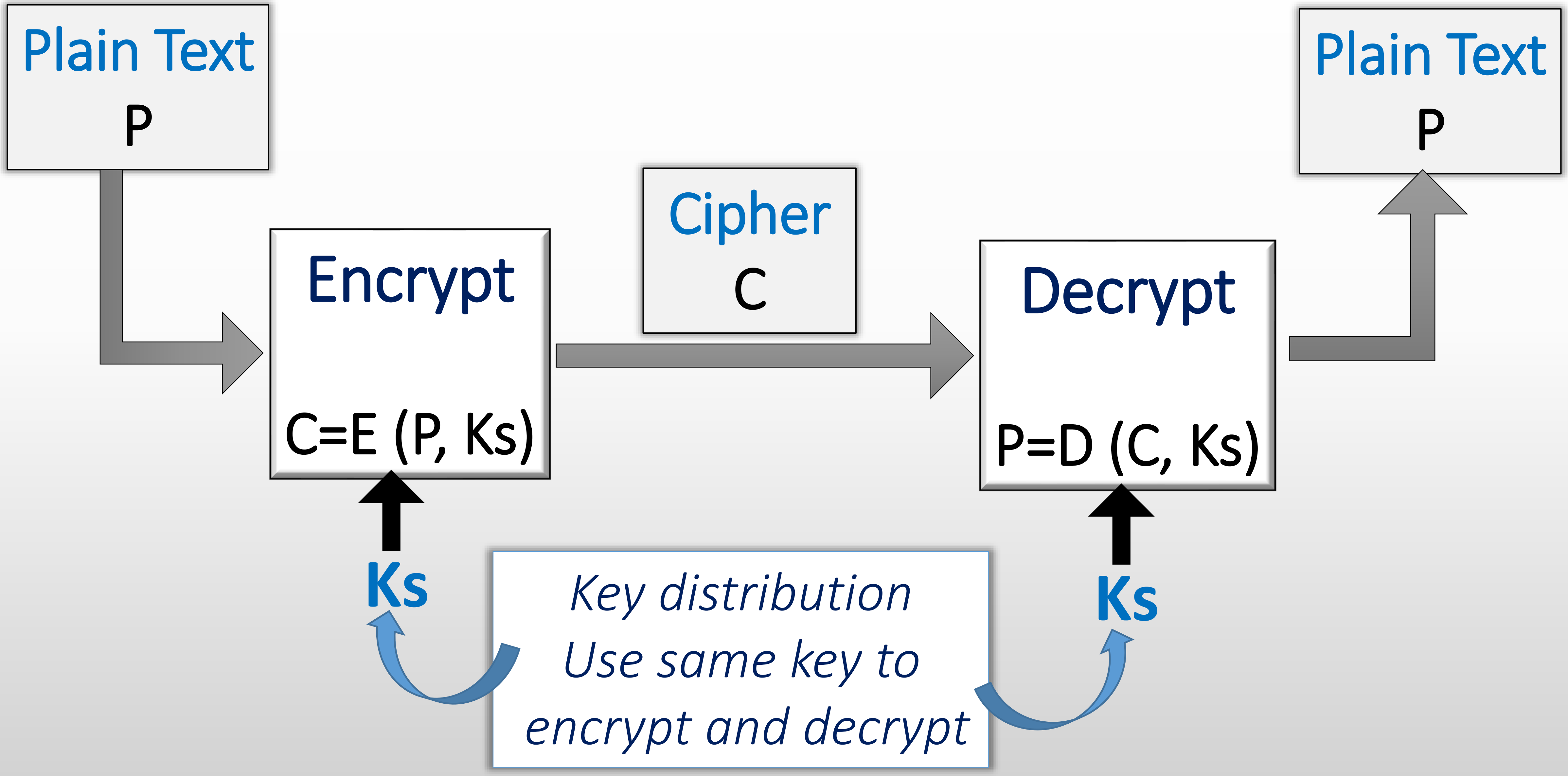


- Same key to encrypt and to decrypt
- Symmetrical Cryptography exist since the Romans
- Encryption and decryption methods is fast and effective
- Encryption/decryption methods can be secret, **or open**
- Does not really handle well multiple users

  (each communication need a private key)
- Limitation highlighted by famous code breakers

  (Alan Turing and the enigma)
- Still very important technology: DES, AES,…….

Symmetrical Cryptography



Symmetrical Cryptography: Traditional methods

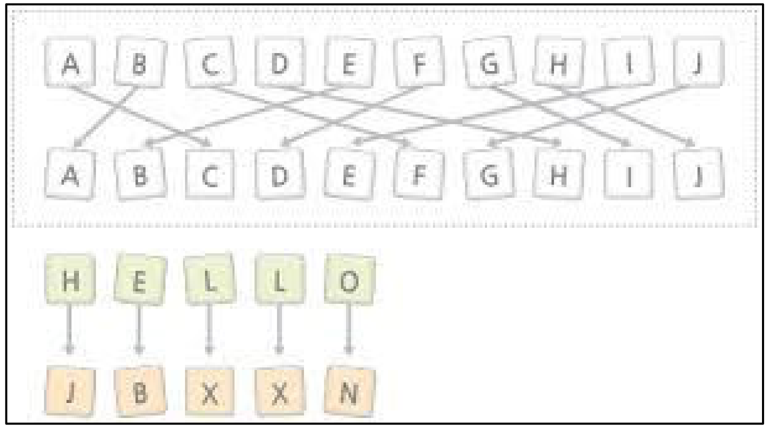
Caesar - Substitution Cipher:

A B C D E F G H I J K .....
D E F G H I J K L M N ....

Diffuse = Substitution + Transposition

Confuse = Successful diffusions

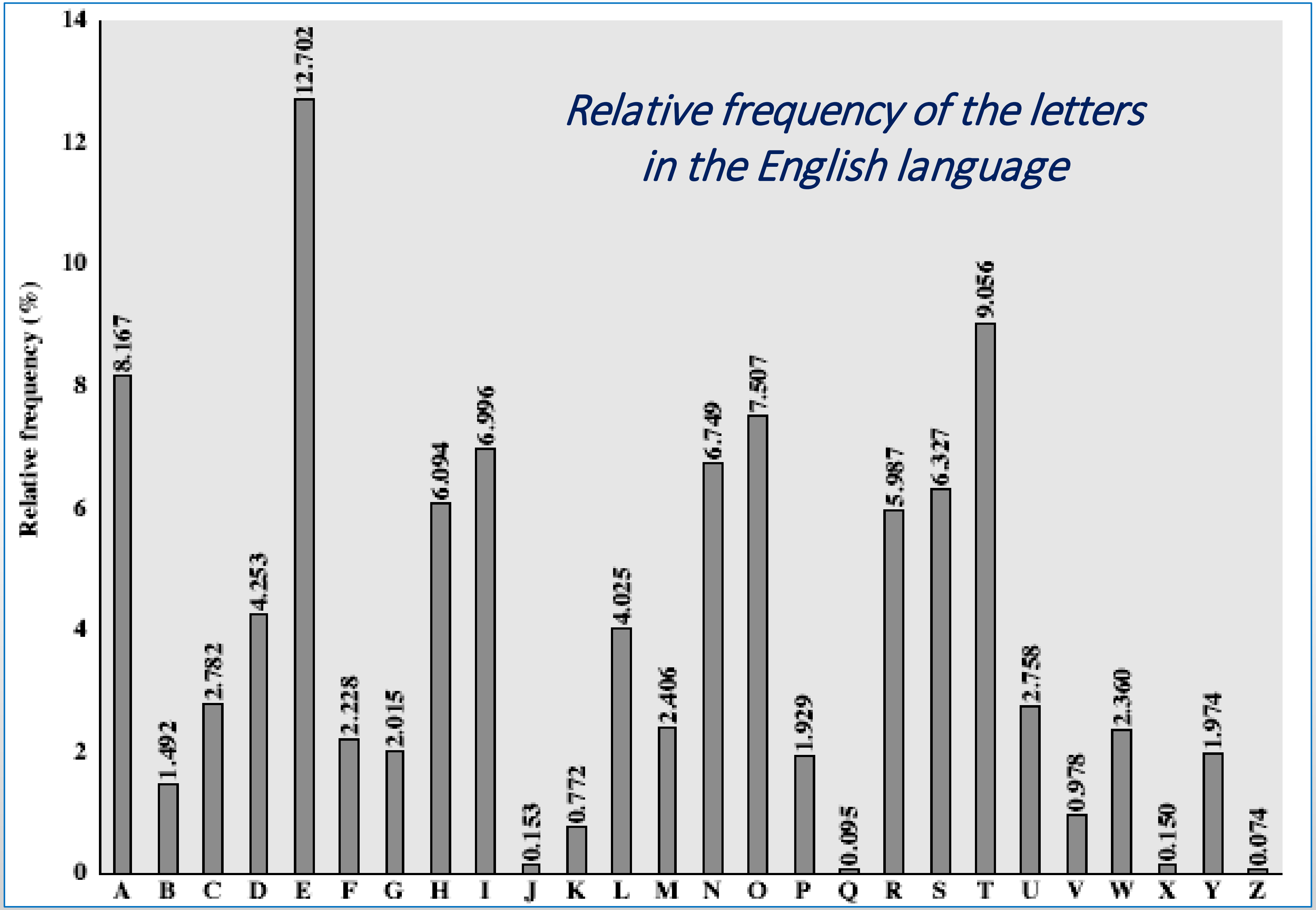
Transposition Cipher:



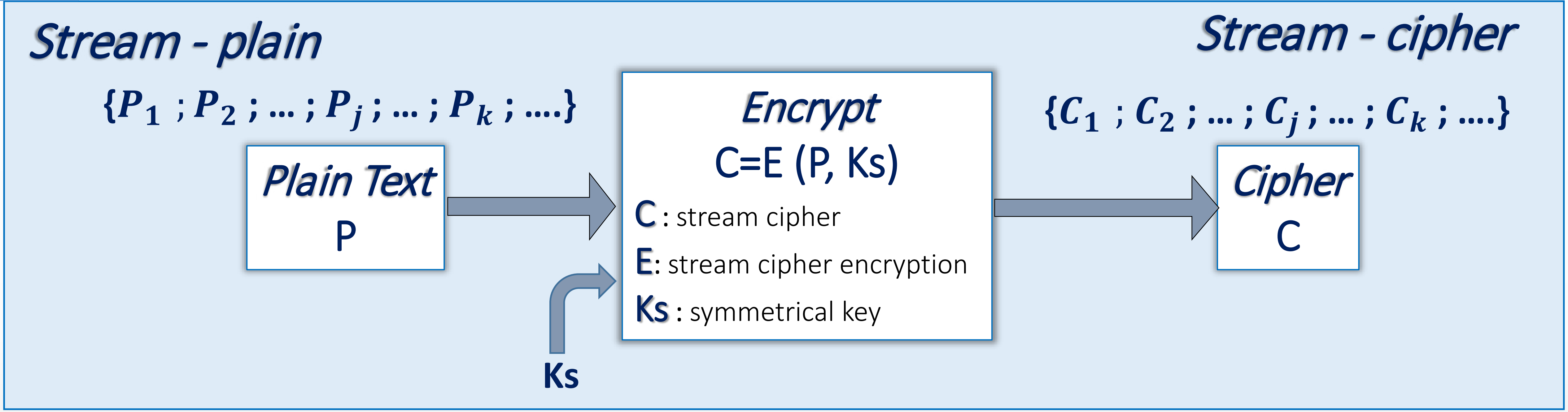
Complex Substitution - Vigenere Cipher

0 A B C D E F G H I J K .....
1 B C D E F G H I J K L .....
2 C D E F G H I J K L M ....
3 D E F G H I J K L M N ....
4 E F G H I J K L M N O ....
5 F G H I J K L M N O P ....
....
25 Z A B C D E F G H I J.......

Frequency analysis



Stream cipher: continuous encryption

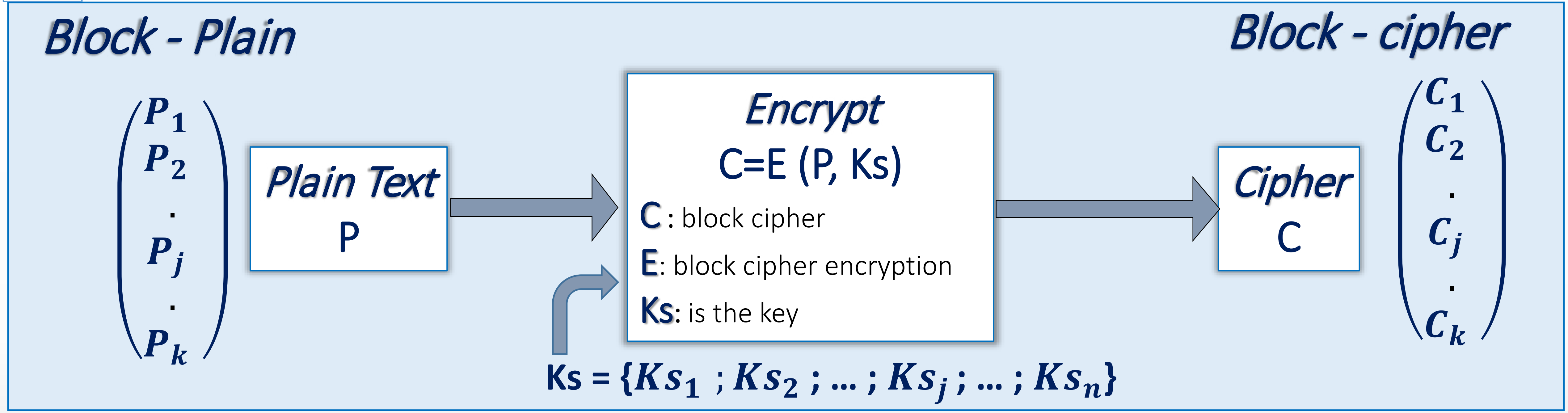


- All elements of the plain text are encrypted with the same algorithm:

$$\boldsymbol{C_i} = E(\boldsymbol{P_i}, Ks);$$

- Data stream “P” is converted in a sequential way to a cypher “C”
- Caesar cipher is an example of stream cipher

Block cipher: block by block encryption



- The encryption is done block by block, not bit by bit
- There is direct link between one single entry bit to one single output bit
- The encryption key is a data stream of length *n*: *Ks* = $\{Ks_1 ; Ks_2 ; ... ; Ks_j ; ... ; Ks_n\}$
- Three cases: *n=k* ; *n>k* ; *or n<k*
- Can be symmetrical or asymmetrical
- Examples of block ciphers includes DES, AES, and RSA.

Block cipher

First k elements of the stream

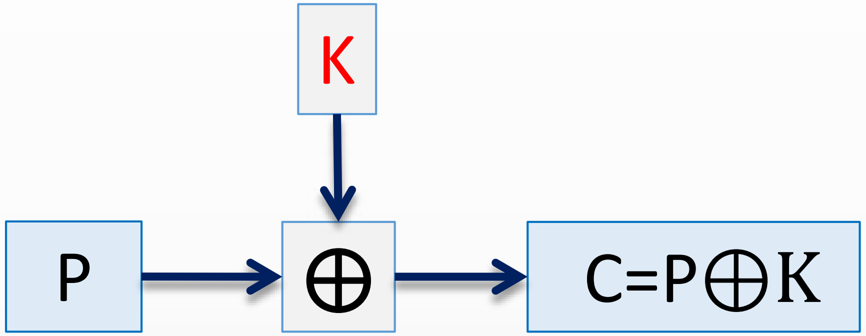
Plain	$p_{11}; p_{12};\dots; p_{1j}\ ;\dots; p_{1k};\dots; p_{i1}; p_{i2};\dots; p_{ij}\ ;\dots; p_{ik};\dots; p_{m1}; p_{m2};\dots\ ; p_{mj}\ ;\dots; p_{mk}$
Key	$[k_1; k_2;\dots; k_j\ ;\dots; k_n]$ $[k_1; k_2;\dots; k_j;\dots; k_n]$ $[k_1; k_2;\dots;\ k_j\ ;\dots; k_n]$
Cipher	$c_{11}; c_{12};\dots;\ c_{1j}\ ;\dots; c_{1k};\dots;\ c_{i1}; c_{i2};\dots\ ;\ c_{ij}\ ;\dots; c_{ik};\dots;c_{m1}; c_{m2};\dots; c_{mj}\ ;\dots; c_{mk}$

- The data stream of the plain text P are grouped into blocks having the same length "*k*"
- The subgroups of *k* bits, or blocks are encrypted together:

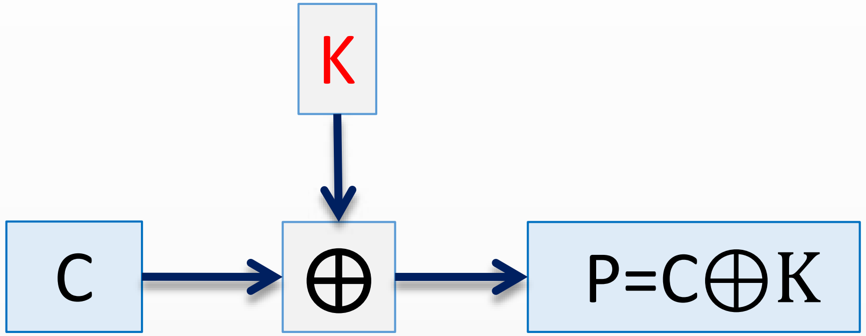
$$\{C_{i1}\ ; C_{i2}\ ; \dots ; C_{ij}\ ; \dots ; C_{ik}\} = \mathrm{E}\ (\{P_{i1}\ ; P_{i2}\ ; \dots ; P_{ij}\ ; \dots ; P_{ik}\}, \mathrm{Ks})$$

XOR Encryption

Encryption



Decryption



$$C \oplus K = (P \oplus K) \oplus K = P$$

XOR	0	1
0	0	1
1	1	0

Key	K	0	0	1	1	…
Plain Text	P	0	1	0	1	…
Cypher	$C=P \oplus K$	0	1	1	0	…
Decrypt	$P=C \oplus K$	0	1	0	1	…

One time pad

k elements of the stream

Plain $p_{11}; p_{12};...; p_{1j} ;...; p_{1n};...; p_{i1}; p_{i2};...; p_{ij} ;...; p_{in};...; p_{m1}; p_{m2};... ; p_{mj} ;...; p_{mn}$

Key $[k_1; k_2;...; k_j ;...; k_n]$ $[k_1; k_2;...; k_j;...; k_n]$ $[k_1; k_2;...; k_j ;...; k_n]$

Cipher $c_{11}; c_{12};...; c_{1j} ;...; c_{1n};...; c_{i1}; c_{i2};... ; c_{ij} ; ...; c_{in}; ...;c_{m1}; c_{m2}; ...; c_{mj} ;...; c_{mn}$

$$\{C_{i1} ; C_{i2} ; ... ; C_{ij}; ... ; C_{in}\}=\{P_{i1} \oplus k_1; P_{i2} \oplus k_2 ; ... ; P_{ij} \oplus k_j; ... ; P_{in} \oplus k_n\}$$

2. Introduction to cryptography

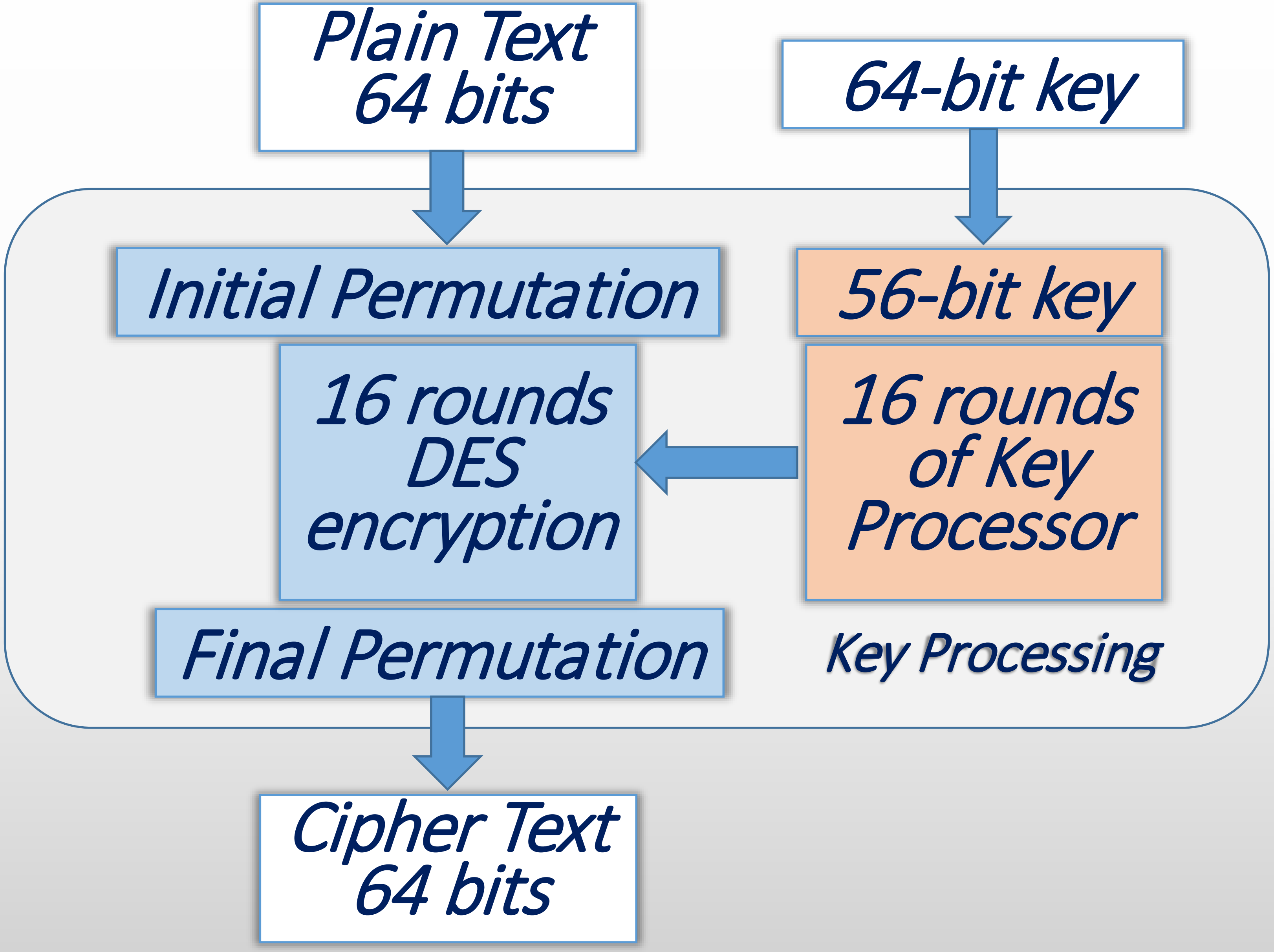
- 1- Definitions
- 2- Symmetrical cryptography
- 3- Data Encryption Standard (DES)
- 4- Advanced Encryption Standard

Data Encryption Standard (DES)

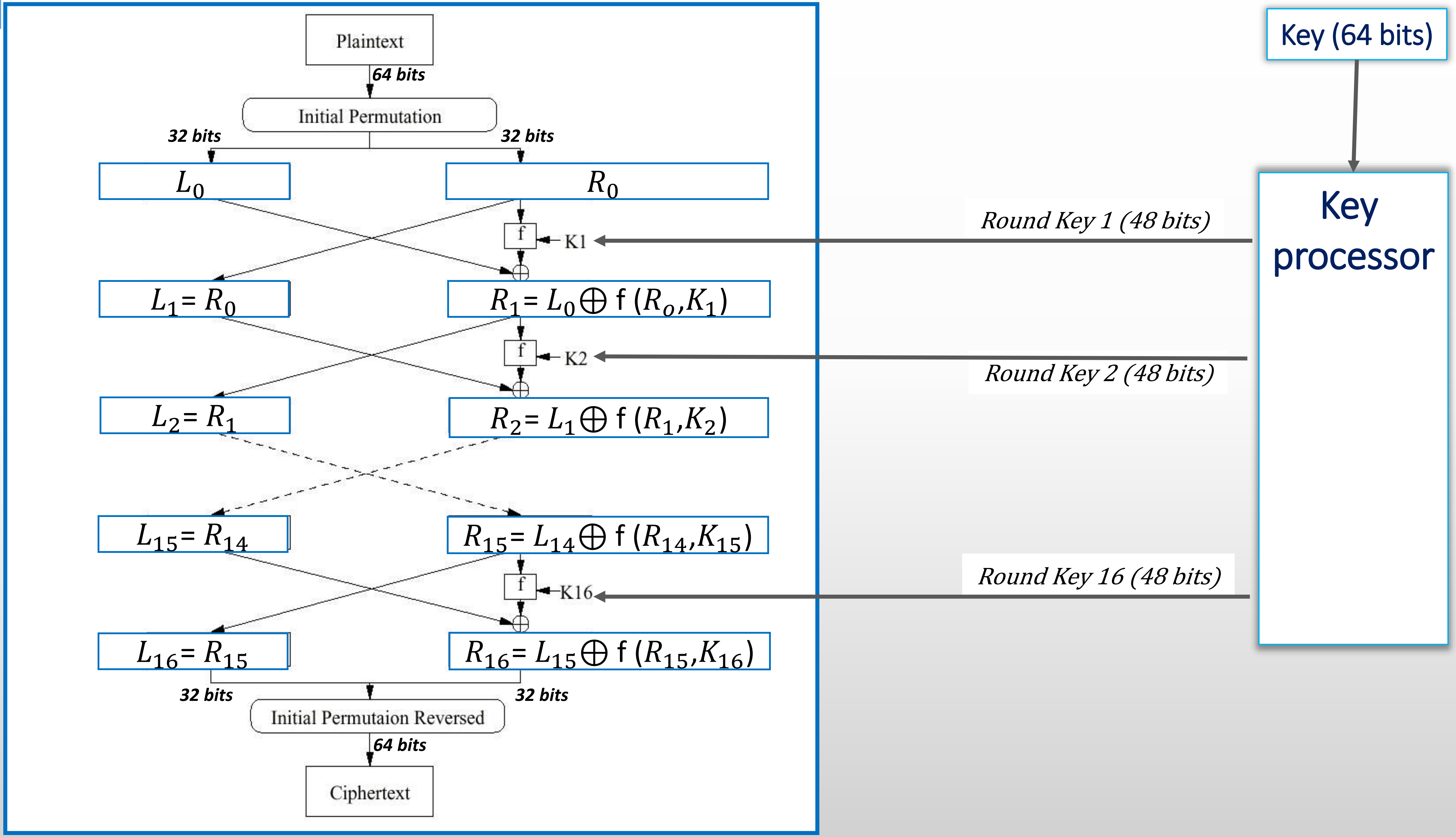
- Developed by IBM early 1970s for the government
- Adopted in 1976 for commercial use, and declassified
- DES operate on block of 64-bits with a 64-bit key (56-bits usable)
- Data manipulation include Feistel work:
  - Diffusion, permutation
  - Logic functions: XOR, AND, OR
  - Repeat 16 times

Modern computers can break DES!!!

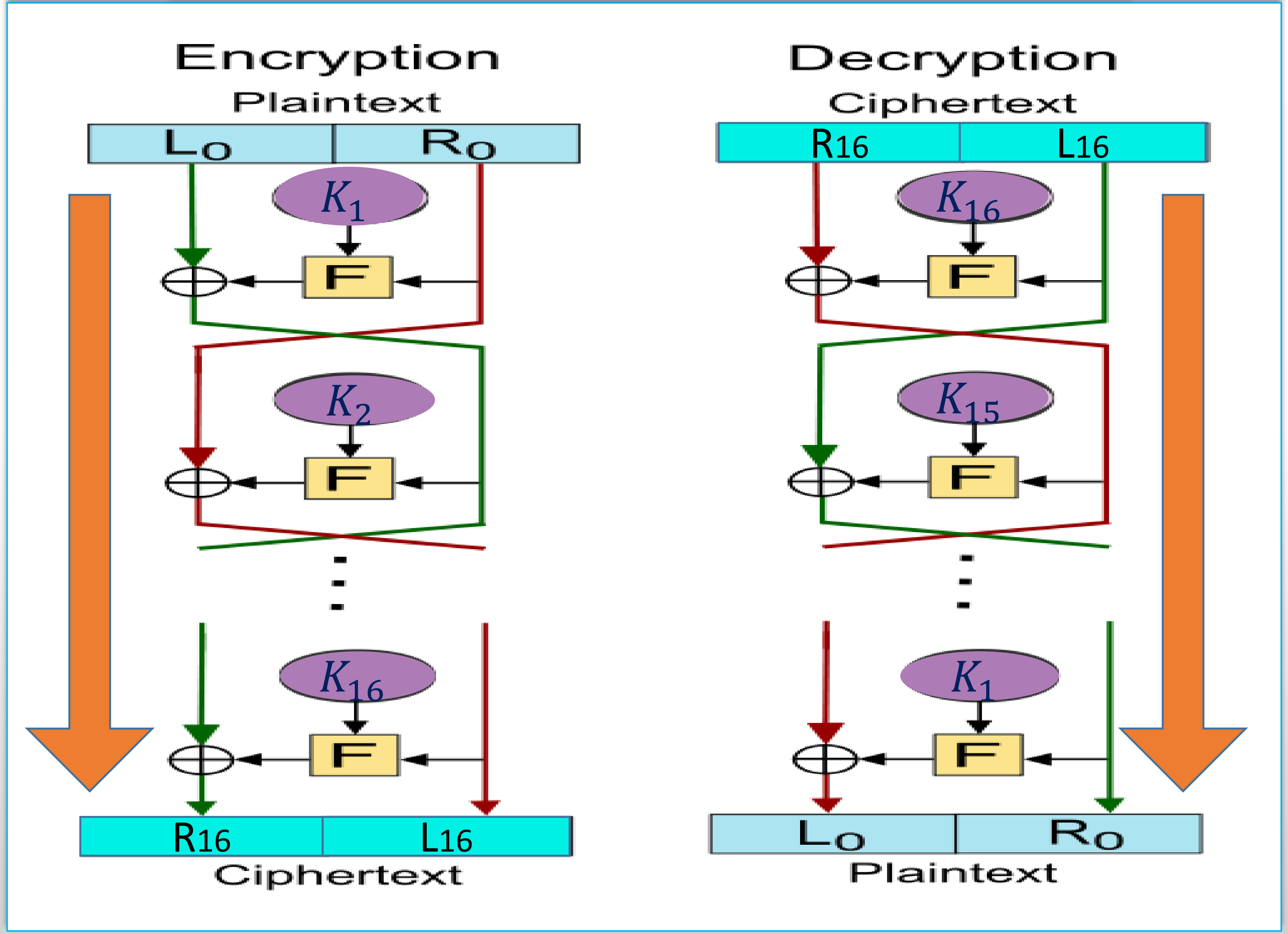
Overview of DES



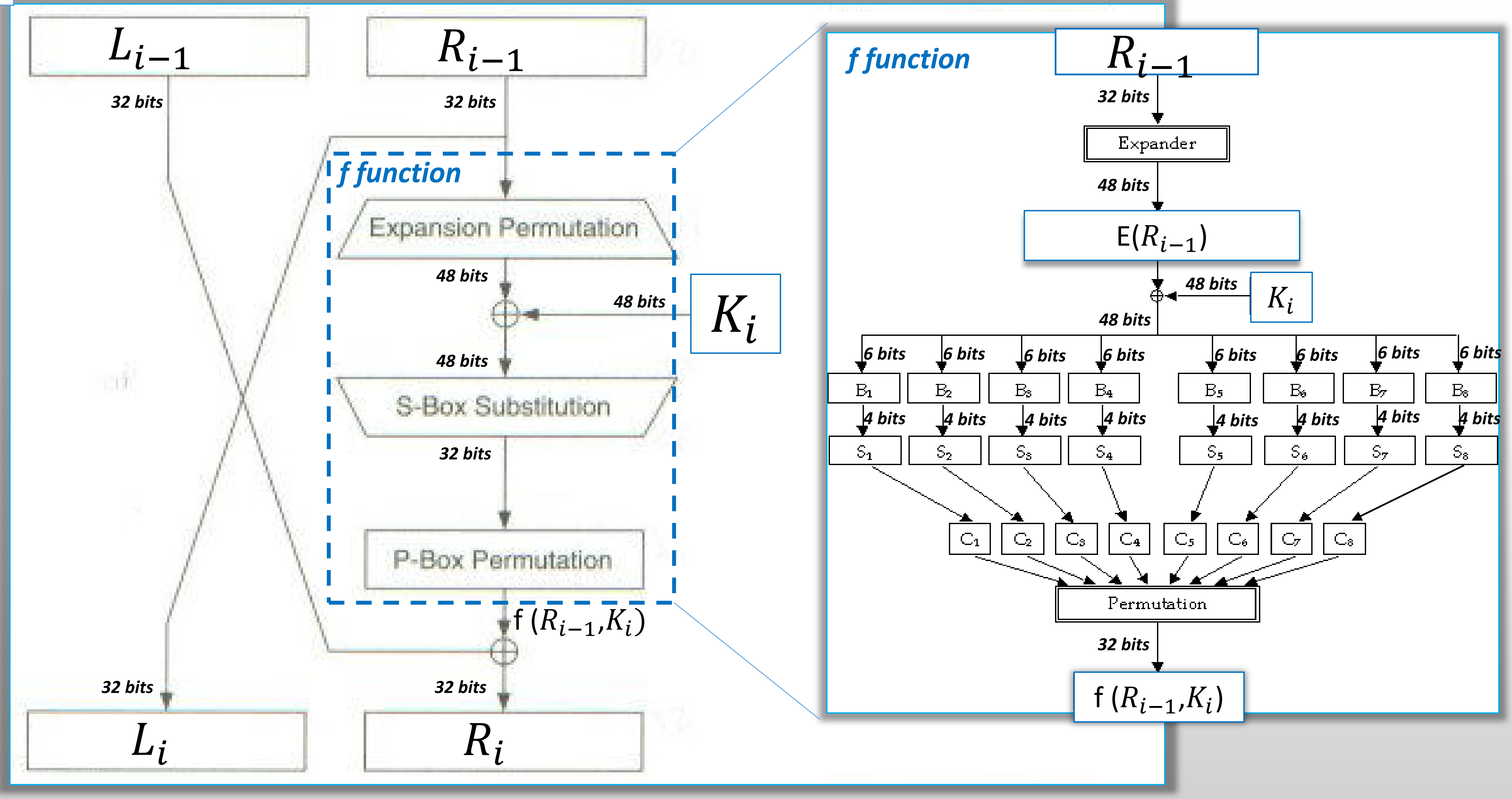
DES: 16 rounds of Feistel encryption



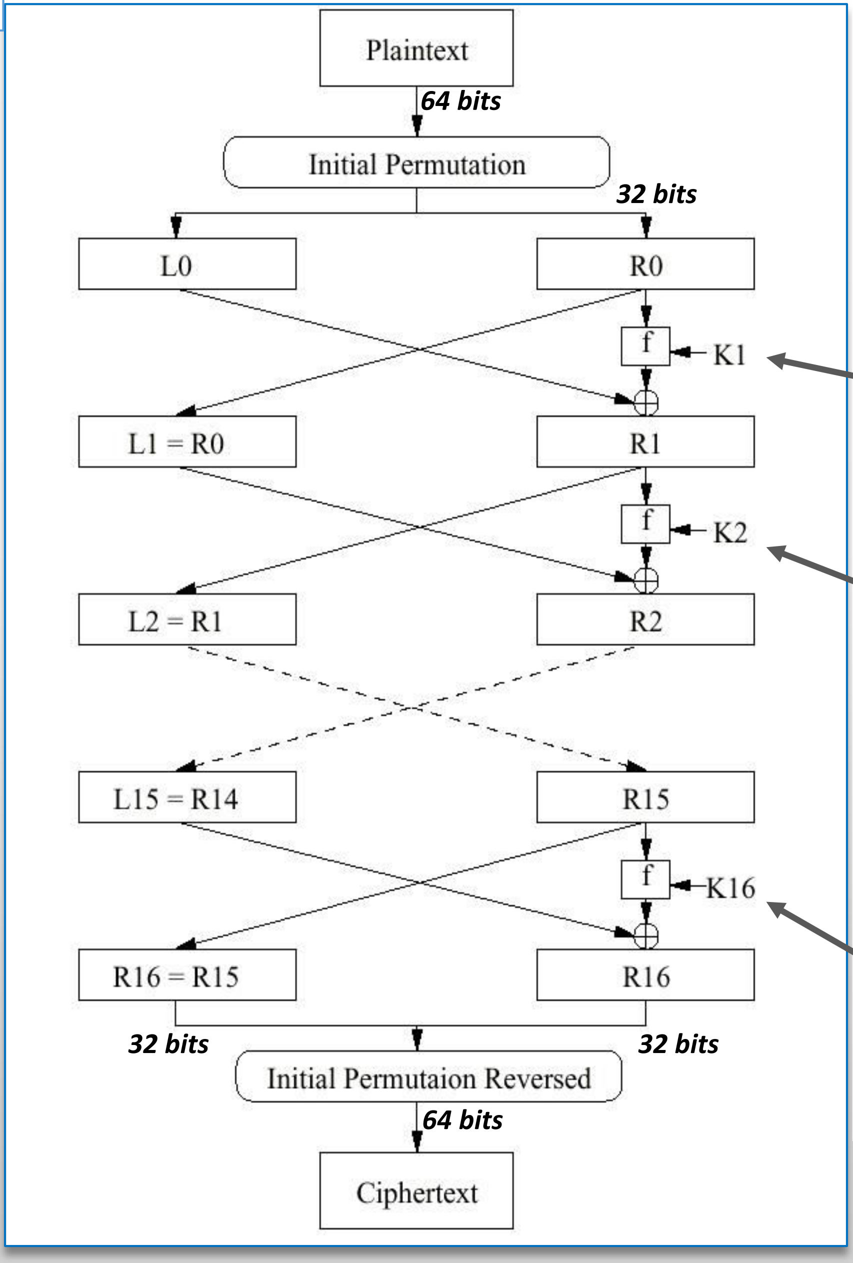
DES is symmetrical (Layer by layer)



DES: description of the f function

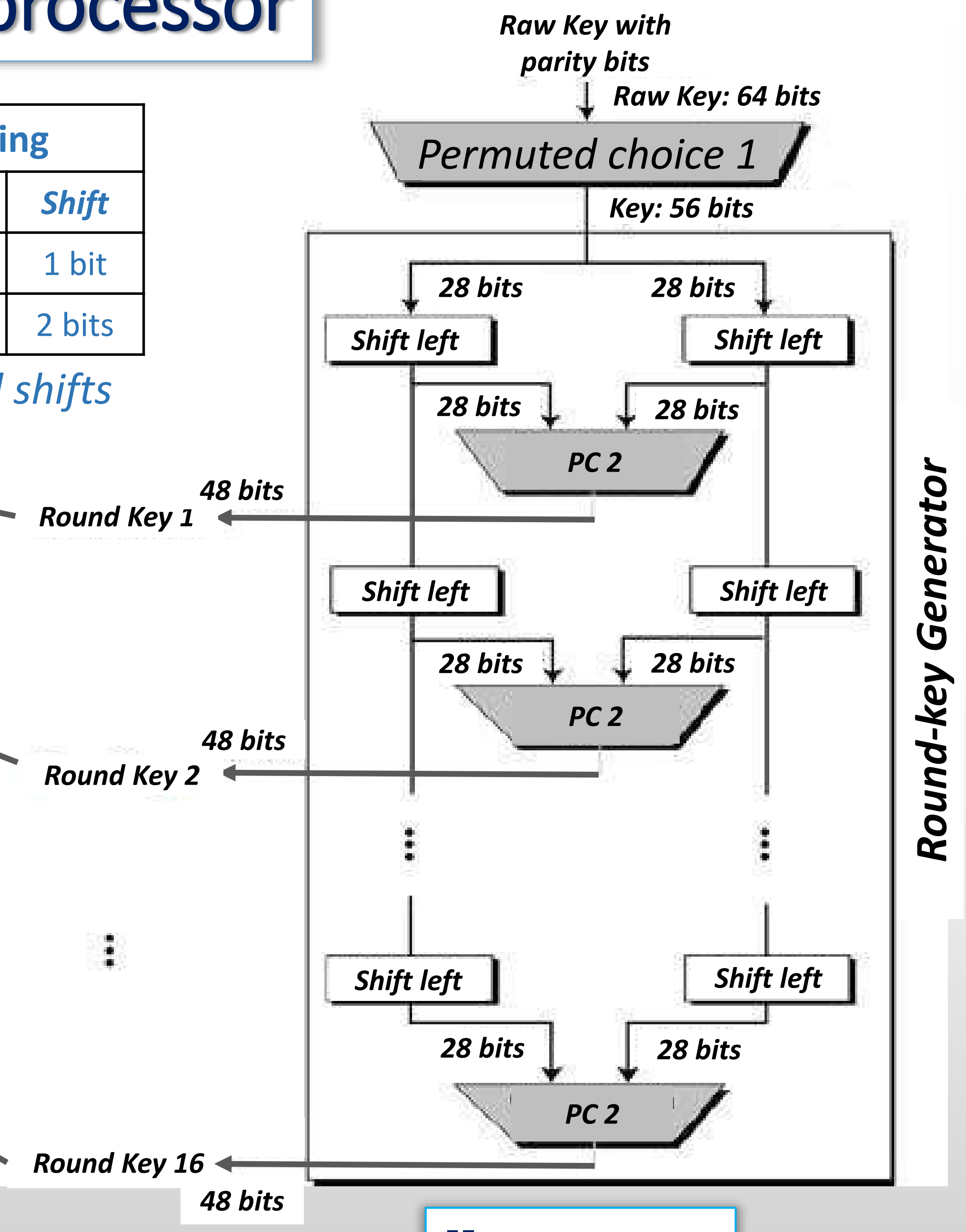


DES: 16 key processor



Shifting	
Round	*Shift*
1, 2, 9, 16	1 bit
others	2 bits

28 total shifts

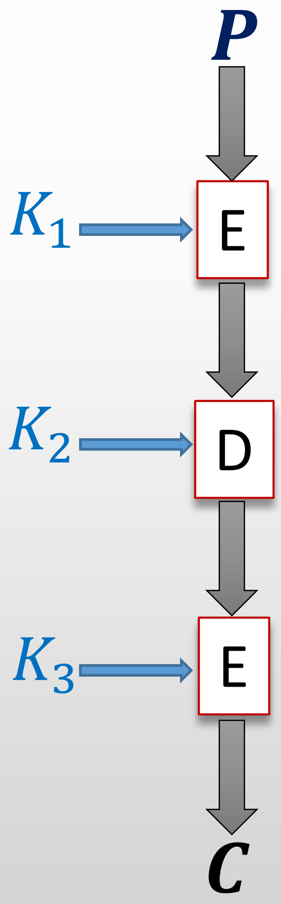


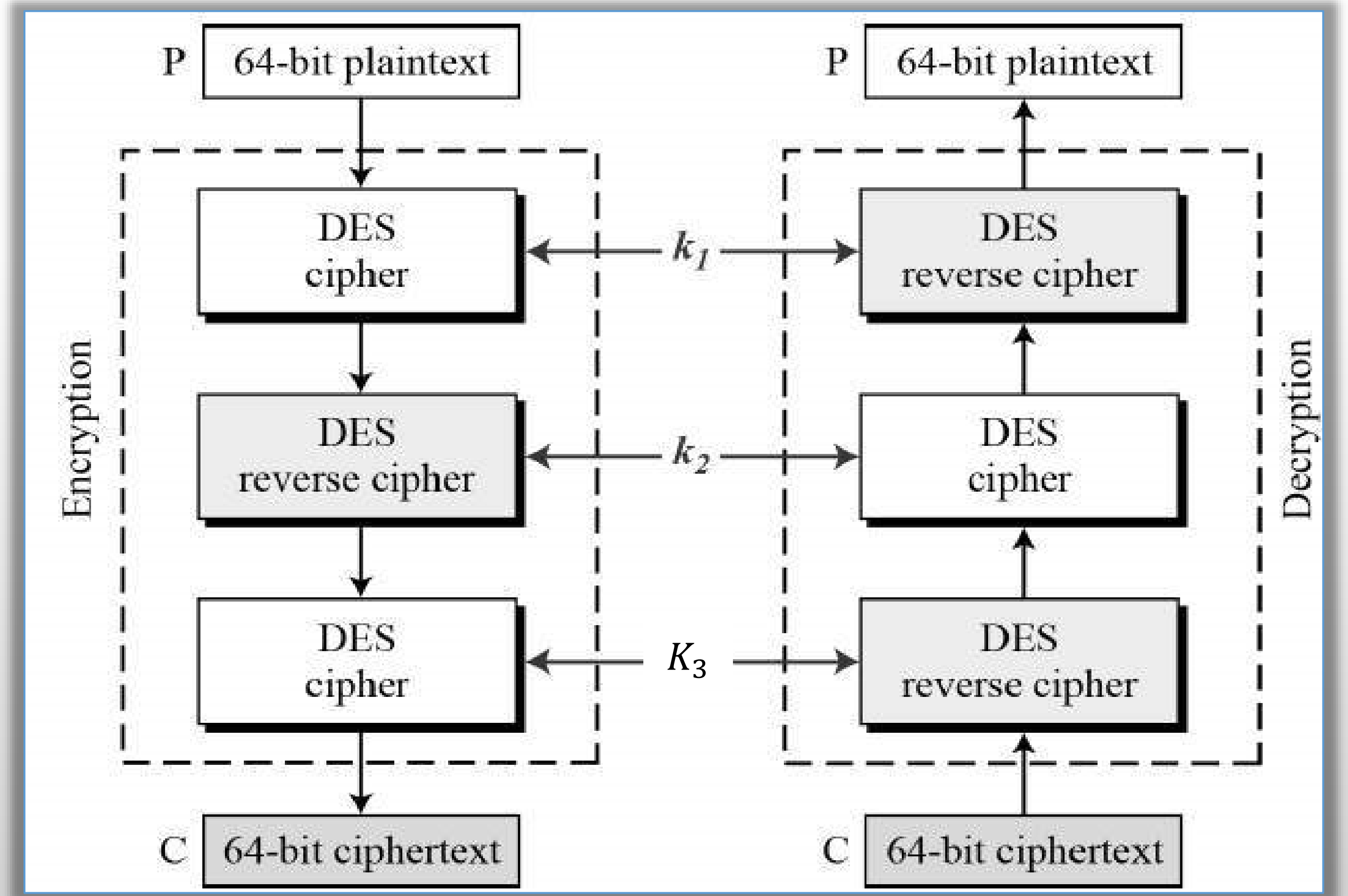
Key processor

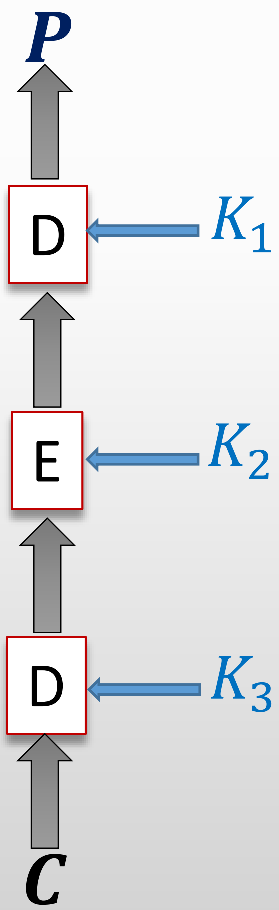
Triple DES chain cipher

$$C = E[D\{E(P, K_1), K_2\}, K_3]$$

$$P = D[E\{D(C, K_3), K_2\}, K_1]$$







Triple DES – Performance comparison

Method	*Properties*	*Strength*
DES	One 56-bit key	Weak
Double DES	Two 56-bit keys	2 X as strong as DES
Two-Key Triple DES	Two 56-bit keys	16 million times as strong as DES
Three-Key Triple DES	Three 56-bit keys	10^{17} as strong as DES
AES	128-bit key	$4\ 10^{21}$ as strong as DES

2. Introduction to cryptography

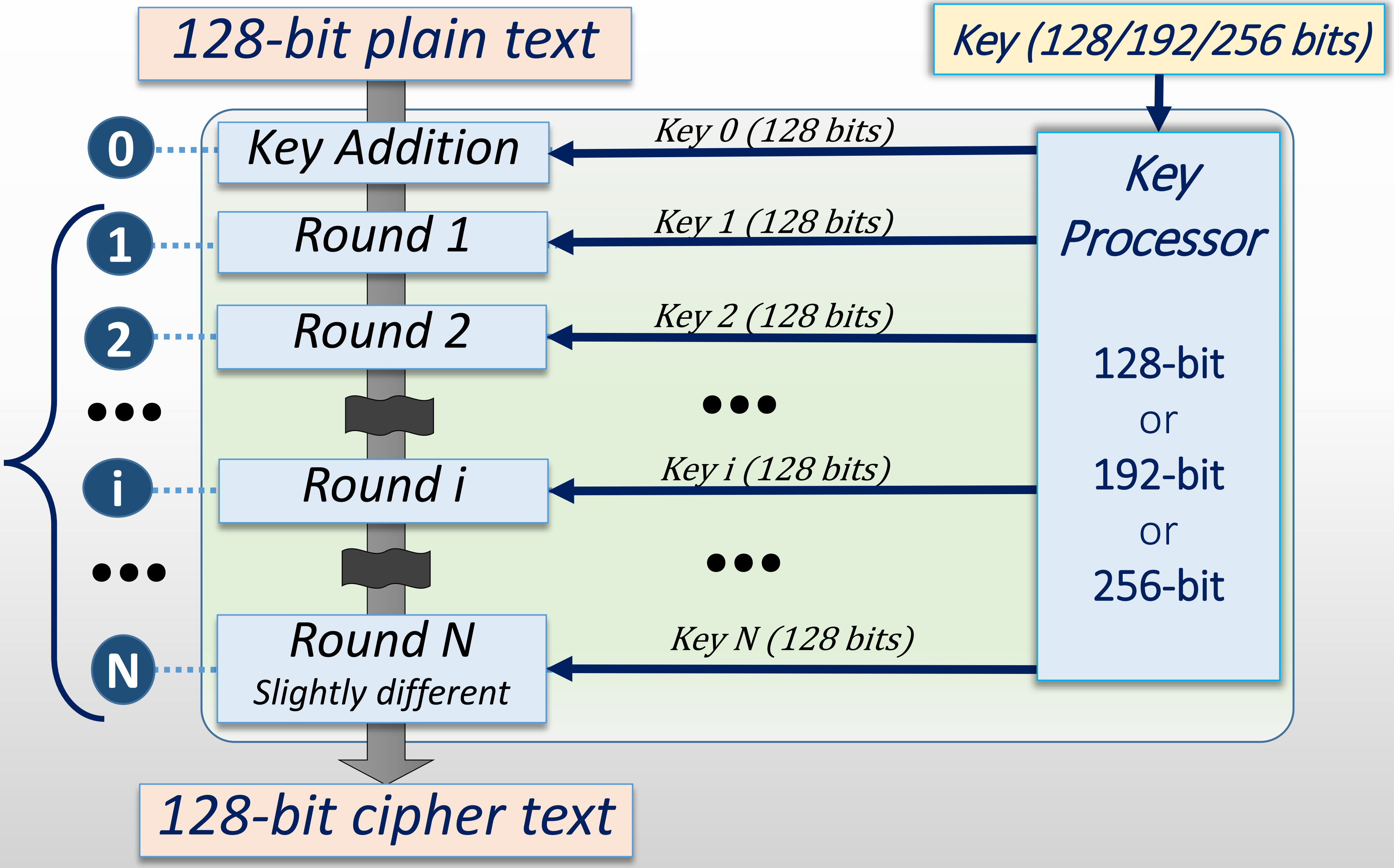
- 1- Definitions
- 2- Symmetrical cryptography
- 3- Data Encryption Standard
- 4- Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES)

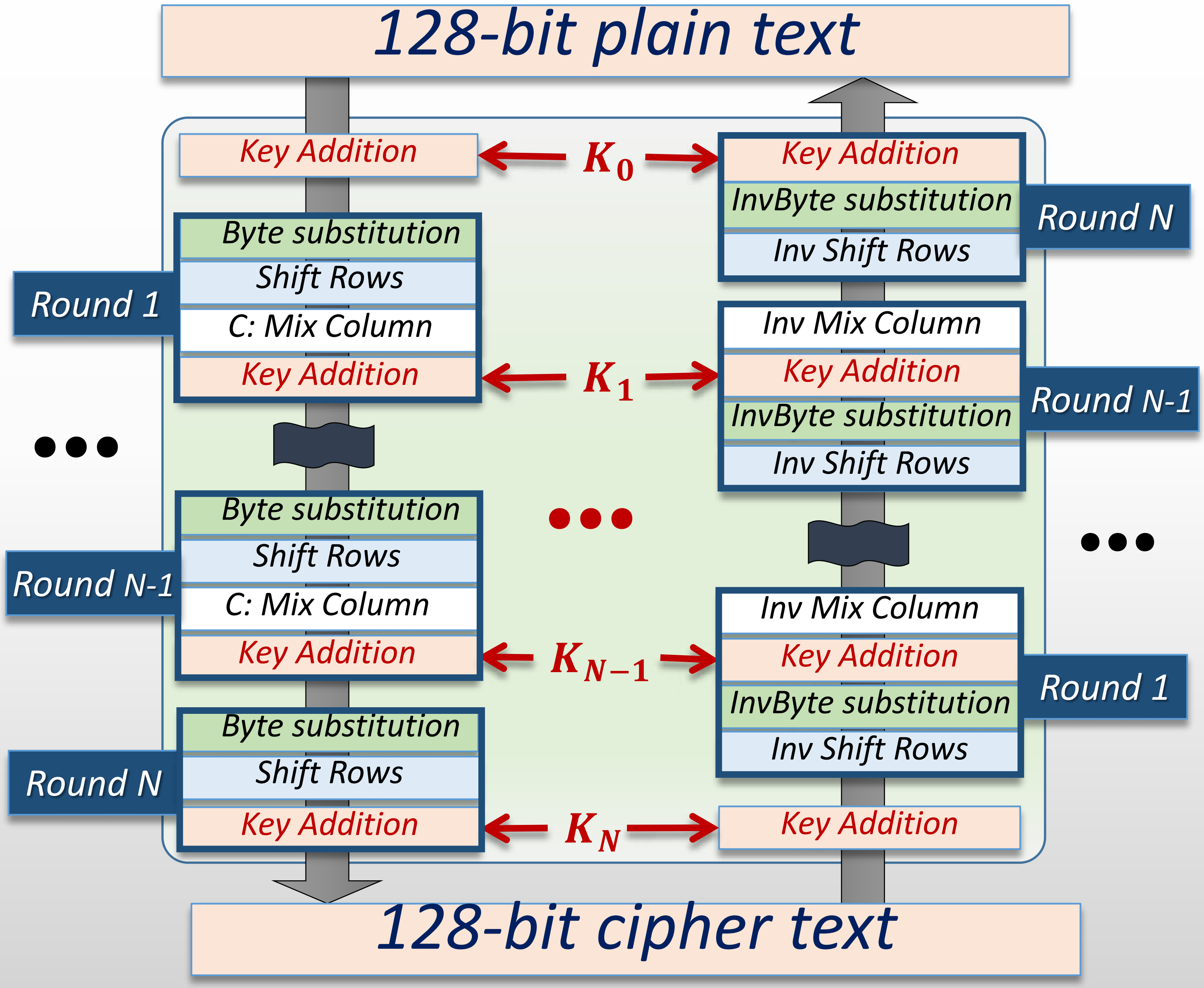
- Developed with the Rijndael algorithm (by V Rijmen & J Daemen)
- Adopted in 2001 for commercial use, and declassified
- AES operate on block of 128-bits with several keys: 128, 192, 256
- Data manipulation include:
  - Diffusion, permutation, shift, mixing
  - Logic functions: XOR, AND, OR
  - Repeat 10, 12, 14 times
- Performance: 4 10^{21} as strong as DES for 128-bit key

Summary AES

Key size	Number of rounds N
128	10
192	12
256	14



AES: Encryption versus Decryption



Use extended Galois Field arithmetic

4 steps per round (not the last one)

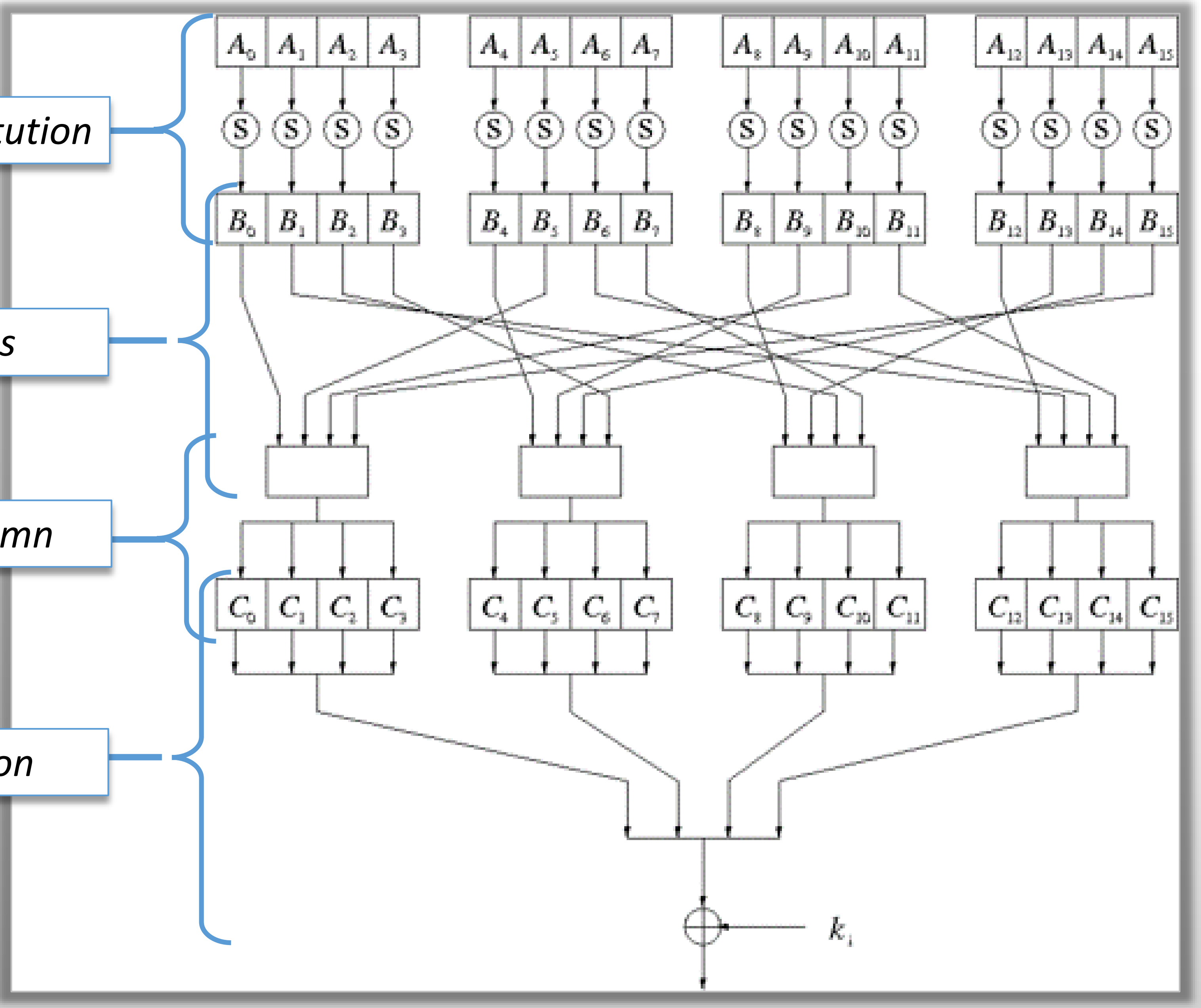
1. Substitution by byte (core of the encryption)
2. Shift rows (Transposition: re-arrange)
3. Mix Columns (Substitution &Transposition)
4. Add round key (XOR)

3 steps for the last round

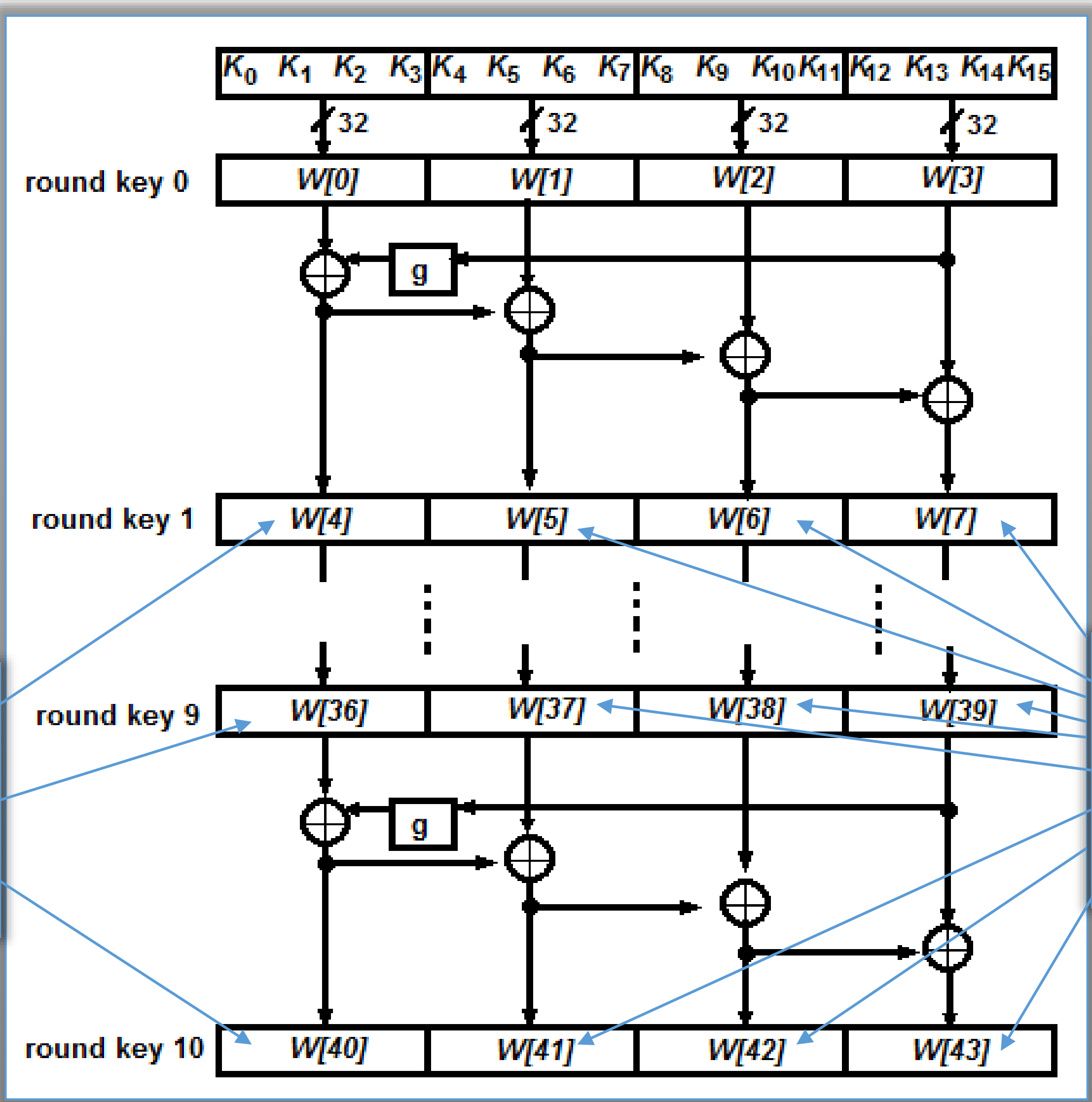
1. Substitution by byte (core of the encryption)
2. Shift rows (Transposition: re-arrange)
3. Mix Columns (Substitution &Transposition)
4. Add round key (XOR)

AES: description of each round

1. S: Byte substitution
2. Shift Rows
3. C: Mix Column
4. Key Addition



AES: Key schedule for each round for 128-bit size



For the left-more word
of sub-key
$i \in \{1 \text{ to } 10\}$
$W(4i) = W(4(i-1)) \oplus g(W(4i-1))$

For the other 3 words
of sub-key
i ; $j = 1,2,3$
$W(4i+j) = W(4(i-1)+j) \oplus W(4i+j-1)$

Effect of fault injection on AES → not easy

- **Plaintext:** *32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34*

  128-bit key: *2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c*

  Ciphertext: *39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32*

- **One fault in the plaintext:** *3**0** 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34*

  Results in the ciphertext: ***c0 06 27 d1 8b d9 e1 19 d5 17 6d bc ba 73 37 c1***

- **One fault in the key:** *2**a** 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c*

  Results in the ciphertext: ***c4 61 97 9e e4 4d e9 7a ba 52 34 8b 39 9d 7f 84***

A single-bit error results in a totally scrambled output

Issues with AES

- **Almost 20 year old**
- **Sensitive to frequency analysis**
  - Plain text is encrypted 128 bit at the time with the same key
  - Very long plain text give an opportunity to crypto-analyst
- **Collisions were reported on the Keys:**
  - Key size of 128 bits → 64 bits **Not safe**
  - Key size of 256 bits → 128 bits **Questionable**
- **Alternate encryption methods based on chaos, and random elements**

DES versus AES

	DES	AES
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers

Form	Properties	Strength
DES	One 56-bit key	Weak
Double DES	Two 56-bit keys	2 X as strong as DES
Two-Key Triple DES	Two 56-bit keys	16 million X DES
Three-Key Triple DES	Three 56-bit keys	10^{17} X DES
AES	128-bit key	4 10^{21} X DES

Key length versus compute time

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Reference	Magnitude
Seconds in a year	$\approx 3 * 10^{7}$
Seconds since creation of solar system	$\approx 2 * 10^{17}$
Clock cycles per year (1 GHz computer)	$\approx 3.2 * 10^{16}$
Binary strings of length 64	$2^{64} \approx 1.8 * 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 * 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 * 10^{77}$
Number of 75-digit prime numbers	$\approx 5.2 * 10^{72}$
Electrons in the universe	$\approx 8.37 * 10^{77}$

Average Time Required for Exhaustive Key Search

Key Size [bit]	Number of keys	Time required at 1 encryption / μs	Time required at 10^6 encryption / μs
32	$2^{32} = 4.3 * 10^{9}$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 * 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 * 10^{38}$	2^{127} μs $= 5.4 * 10^{24}$ years	$5.4 * 10^{18}$ years

Homework #2

Back to back comparison DES versus AES:

- Encryption at each round
- Sub-key generator
- Decryption at each round

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu